IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IPC SYSTEMS, INC.	:	
	:	
Plaintiff	:	
	:	
v.	:	**Case No. _____**
	:	
PATRICK GARRIGAN	:	
	:	
Defendant.	:	

COMPLAINT

COMES NOW Plaintiff IPC Systems, Inc. ("IPC") and files this, its Complaint against Defendant Patrick Garrigan ("Defendant"), and respectfully shows this Honorable Court as follows:

I. INTRODUCTION

1.

This action arises from the theft of IPC's proprietary information and trade secrets by Defendant, IPC's former employee. Upon information and belief, Defendant is now using the information he unlawfully misappropriated from IPC to unfairly compete with IPC. IPC brings this action seeking injunctive relief to restrain and enjoin Defendant's unlawful conduct and to recover damages for the harm he has already caused IPC.

II. PARTIES, JURISDICTION AND VENUE

2.

IPC is a corporation organized and existing under the laws of Delaware. IPC maintains its principal place of business at Harborside Financial Center, Plaza 10, 3 Second Street, 15th Floor, Jersey City, New Jersey 07311.

3.

Defendant is an individual who resides at 199 Twelfth Street, Unit 5, Atlanta, Georgia 30309.

4.

This Court has subject matter jurisdiction over Counts II and III of this Complaint pursuant to 28 U.S.C. § 1331 because these claims arise under federal law. This Court has subject matter jurisdiction over IPC's state law claims pursuant to 28 U.S.C. § 1367.

5.

In the alternative, this Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because IPC is of diverse citizenship from Defendant, and the amount in controversy exceeds $75,000, exclusive of interest and costs.

6.

Venue in this Court is proper pursuant to 28 U.S.C. §§ 1391(a)(2) and (b)(2) because a substantial part of the events or omissions giving rise to the claims in this action occurred in this judicial district. Alternatively, venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(a)(3) and (b)(3) because Defendant is subject to personal jurisdiction in this judicial district.

III. STATEMENT OF FACTS

IPC's Business

7.

IPC provides technology and connectivity solutions to financial market participants in the United States and around the world. IPC's products and services enable the business of the trading and brokerage community.

8.

More specifically, IPC makes and services "turret" communications systems, also called dealerboards, that combine private branch exchanges, data switching, computer telephony, voice recording, and multimedia capabilities. IPC's products are used by financial institutions for voice and data transmission and routing in their trading environments. IPC markets its products directly and through resellers and systems integrators worldwide.

9.

Among other things, IPC has developed and acquired extensive databases of customer and vendor information over many years and at a great expense, which provides IPC with a competitive advantage in selling and providing its products and services.

Defendant's Employment with IPC

10.

Defendant became employed by IPC in 2001.

11.

During the last several years of his employment by IPC, Defendant was based in and operated out of IPC's Southeastern Regional Office located at 11605 Haynes Bridge Road, Suite 575, Alpharetta, Georgia, 30009.

12.

Prior to the end of his employment with IPC, Defendant reported to Brian Garvey, IPC's Vice President of Sales for the Americas. Mr. Garvey reports to Neil P. Fishler, IPC's Vice President of North American Trading Systems Sales.

13.

During the final year of his employment with IPC, Defendant's role was the management and service of IPC's existing customers and conducting of sales to new customers in an assigned territory in the Southeastern United States, as well as in Central and Latin America. Defendant did not have any responsibility for customers who did not have a physical presence in his territory.

14.

As an employee of IPC, Defendant was provided with access to highly confidential and trade secret information relied upon by IPC in conducting its business.

IPC Requires Its Employees to Maintain the Confidentiality of IPC's Confidential and Trade Secret Information.

15.

IPC expressly requires its employees to maintain the confidentiality of IPC's confidential and trade secret information.

16.

IPC's Code of Ethics provides, in pertinent part, that "[i]t is the responsibility of each employee to ensure the proper use and security of all assets provided to them or used by them in the course of IPC's business. IPC employees should take all appropriate action to preserve and protect the confidential and

sensitive information of IPC. All such information must only be used by IPC's employees in furtherance of IPC's business." A true and correct copy of IPC's Code of Ethics is attached hereto as **Exhibit 1.**

17.

IPC's Code of Ethics was distributed to, reviewed, and acknowledged by Defendant, most recently on May 17, 2010.

18.

Additionally, IPC's Trade Secrets Policy, distributed to and acknowledged by all IPC employees in February 2006, provides:

> The business and operations of [IPC], and its subsidiaries and affiliates (collectively, "IPC" or the "Company") involve valuable, confidential and proprietary information known as "Trade Secrets." Under federal and state law, a Trade Secret is any formula, pattern, device or compilation of information that (i) is used in a business, (ii) is unknown to others outside that business, (iii) gives the business a competitive advantage, and (iv) is the subject of reasonable efforts to maintain its secrecy. A Trade Secret does not have to be unique or novel; it need only provide a distinct economic advantage to IPC.
>
> The following is a list of items that qualify as IPC Trade Secrets:
>
> - The names of IPC's customers
> - The names and qualifications of IPC's development partners and/or contractors
> - Any aspect or description of IPC's relationship with its customers, e.g., product or service purchases, pricing policies, price lists, discounts, orders and revenue

- Computer systems, software (object code and source code) and databases
- Internal specifications, technical processes, testing procedures, diagrams, designs drawings, models, and any other techniques, developments, improvements, inventions, and processes that are, or may be, produced in the course of IPC's engineering or other operations
- Marketing development and research plans
- Manufacturing processes or techniques
- Financial, accounting, recruiting and legal information
- Any other information not generally and publicly know regarding IPC or its operations, products, suppliers, markets, sales, costs, profits or customers, or other information acquired, disclosed or made known to any employees or agents during the course of their employment or agency that, if used or disclosed, could adversely affect IPC's business or give its competitors a commercial or economic advantage.

A true and correct copy of IPC's Trade Secrets Policy is attached hereto as **Exhibit 2**.

19.

IPC's Trade Secrets Policy also provides, in relevant part:

To prevent the harmful disclosure of Trade Secrets to its competitors, IPC requires all employees, consultants, contractors and other representatives of the Company (each an "Employee") to adhere to the following:

1. Each employee owes IPC a high duty of loyalty. No employee may, during or after his or her employment with IPC, use any Trade Secrets for his or her benefit or disclose any Trade Secrets to any person or business, without the prior written consent of the IPC General Counsel.

…

> 6. Upon termination of employment or at IPC's request, each Employee shall promptly return to the Company all memoranda, notes, records, reports, technical manuals, and any other documents (and all copies thereof) in his or her possession, custody, or control relating to the trade secrets.

See **Exhibit 2**.

IPC Spends Significant Time, Effort, and Money Developing, Maintaining and Protecting its Trade Secrets and Confidential Information.

20.

IPC makes substantial efforts to ensure that documents and electronically stored information containing IPC's confidential and trade secret information cannot be easily accessed by the public or IPC's competitors

21.

User names and passwords are required for IPC's employees to access electronically stored information residing on its information technology systems.

22.

The network on which IPC's information is stored is protected from outside interference or access by two firewalls that are managed by IPC.

23.

IPC employees who are authorized users of the IPC network must log in using a company-provided login ID and password.

24.

With respect to IPC's email system, in addition to typical login credentialing, IPC runs two additional security components. First, all inbound and outbound email correspondence pass through Mx Logic, a managed email protection system that prevents spam, viruses, worms, malicious content and attachments, and other harmful email threats from passing into or out of IPC's email system. Second, IPC utilizes Dell Secureworks, an intrusion detection system which monitors IPC's network and email systems for suspicious activity, potentially harmful use, and unauthorized access.

25.

Electronic access cards are also necessary for employees to access IPC's offices.

26.

IPC also uses Salesforce.com to track sales opportunities and for other sales and marketing purposes.

27.

IPC employees input information about contacts with customers and prospective customers into the Saleforce.com database.

28.

The information contained in Salesforce.com is also highly valuable and proprietary to IPC and has been gathered at significant cost to IPC.

29.

A user name and password issued by IPC is required for IPC employees to access IPC's data in Salesforce.com. Access to IPC's Salesforce.com website is restricted to only those IPC employees who require access to further their sales efforts. IPC further has its own security modules to prevent unauthorized use of Salesforce.com.

30.

As an account manager, Defendant was provided a password and user name so that he could access the Salesforce.com website and IPC's proprietary, confidential, and trade secret information on the website in furtherance of IPC's business.

The End of Defendant's Employment with IPC and his Subsequent Employment with a Competitor

31.

On October 12, 2011, Mr. Fishler met with Defendant at IPC's Alpharetta, Georgia office.

32.

During their meeting on October 12, 2011, Defendant did not discuss with Mr. Fishler a need or desire to obtain information concerning IPC's customer base throughout North America. Moreover, during their meeting, Defendant never mentioned to Mr. Fishler that Defendant had requested or intended to request such a report.

33.

Defendant did not have any legitimate reason to obtain information concerning all of IPC's customers in North America for his meeting with Mr. Fishler or otherwise. Nothing Defendant and Mr. Fishler discussed during their meeting on October 12, 2011, required Defendant to obtain access to such a report.

34.

On or about October 28, 2011, and employee in IPC's Alpharetta, Georgia office discovered in that office an October 26, 2011 facsimile result report (the "Facsimile Report") showing that Defendant had submitted a Candidate Release Authorization to IPC's competitor Siemens Enterprise Communications, Inc. ("Siemens"), a subsidiary of the large, multi-national company, Siemens AG. A true and correct copy of the October 26, 2011 Facsimile Report is attached hereto as **Exhibit 3**.

35.

Siemens is a direct competitor of IPC and is looking to aggressively expand its presence in the market for communications systems for the financial services industry.

36.

The Facsimile Report was then forwarded by the employee who discovered it to Mr. Garvey who then sent it to Mr. Fishler.

37.

After Mr. Fishler received the Facsimile Report on October 28, 2011, he spoke with Defendant several times by telephone and then met with Defendant on November 3, 2011, at IPC's Alpharetta, Georgia office to discuss whether Defendant was interested in continuing his employment with IPC.

38.

In Mr. Fishler's initial conversations with Defendant, Defendant denied that he was interviewing with Siemens or that he was leaving IPC to become employed by Siemens. However, during their November 3, 2011 meeting, Defendant admitted to Mr. Fishler that he had received an offer from Siemens with national sales responsibilities in the financial services vertical. Defendant also advised Mr. Fishler that he was likely to accept the offer.

39.

Defendant left the meeting with Mr. Fishler and never returned to work at IPC.

40.

In the weeks leading up to and at the time he resigned from IPC, Defendant removed items from his personal office at IPC's Alpharetta, Georgia office, leaving only several personal effects at the time of his resignation.

41.

In the meeting with Mr. Fishler on November 3, 2011, Defendant turned in his IPC-issued computer but did not turn over any documents or electronically-stored information to IPC.

IPC Uncovers Defendant's Theft of IPC's Trade Secrets, and Other Information.

42.

Following the end of Defendant's employment, IPC learned that on October 14, 2011, while still employed by IPC, Defendant requested IPC's Operations Support Systems Coordinator, Susan Merganthaler, to generate and to provide him a report containing highly sensitive trade secret information for IPC's entire customer base across North America (the "Report").

43.

The Report contains information with respect to all of IPC's customers, not just those for whom Defendant was responsible, including name, contact information, the IPC employee responsible for the account, the date IPC's products were installed, the type of products installed, the date IPC most recently serviced the customer, and details concerning exactly what that customer may require in the form of communications solutions.

44.

According to e-mails Defendant sent to Ms. Merganthaler, Defendant claimed to be requesting the Report to provide information to Mr. Fishler and Mr. Garvey.

45.

Defendant did not have a legitimate need for the information contained in the Report, because Mr. Fishler and Mr. Garvey are familiar with the information in the Report, and they did not request or expect Defendant to provide them with any opinions or analysis of the information contained in the Report. Also, during their meeting on October 12, 2011, Defendant and Mr. Fishler did not discuss anything that could have legitimately led Defendant to believe he needed to obtain

the Report in order to follow-up with Mr. Fishler or to otherwise perform his job responsibilities.

46.

To IPC's knowledge, Defendant had never previously requested or obtained a report of this magnitude during his employment with IPC and it was highly unusual for him to do so.

47.

As an Account Manager for certain customers in the Southeastern United States, Central America, and Latin America, Defendant had no legitimate need for the Report and would not have had a valid reason to be in possession of the Report

48.

The only conclusion that can be drawn from Defendant obtaining the Report at the time he did is that he intended to and has misappropriated the Report to use competitively against IPC in his employment with Siemens.

49.

The information in the Report would be of enormous economic value to IPC's competitors. The Report would be extremely valuable to Defendant in his employment in national sales at Siemens because, among other things, it identifies IPC's customers throughout North America and provides information about where

those customers are in their technology cycle. This would allow Defendant and Siemens to strategically target their sales efforts towards IPC's customers.

50.

Defendant duped Ms. Merganthaler into providing him with the Report by telling her he needed it to provide information to Mr. Fishler and Mr. Garvey; however, Defendant did not need the Report for such purpose.

51.

When Ms. Mergenthaler learned that Defendant had abruptly left IPC's employment and was joining a competitor, she was horrified because she realized she had provided Defendant with extremely sensitive and valuable information concerning ALL of IPC's customers in North America. Ms. Mergenthaler would never have provided the Report to Defendant, if she knew he was planning to leave the company, especially if she knew he was leaving to join a competitor.

52.

Upon information and belief, on the date he obtained the Report, Defendant had already decided to end his employment with IPC and had accepted the position with Siemens, IPC's competitor.

53.

Following the end of Defendant's employment with IPC, IPC also conducted a forensic investigation of Defendant's laptop computer and learned that in the weeks leading up to the end of his employment, Defendant downloaded and printed an enormous amount of highly proprietary information from his IPC laptop computer, much of which constitutes IPC's trade secrets.

54.

IPC's forensic investigation has revealed that in the final week before his resignation from IPC, Defendant printed and downloaded from his IPC-issued computer voluminous documents, files and folders which were IPC's trade secret and confidential information and which IPC spends significant time, effort and money developing, maintaining and protecting. The trade secrets and confidential information Defendant took, in hard copy or electronic form appear to include, but are not limited to:

- customer lists;
- pricing lists;
- quotes IPC had made to existing and prospective customers;
- IPC's installed base;
- costs and margin information;

- product presentations;
- distributor price lists; and
- price and cost estimating tools.

55.

Defendant also transferred from his IPC-issued computer to an external drive the resumes of several IPC employees.

56.

IPC's has also determined that in the final week before from the end of his employment with IPC, Defendant accessed IPC's proprietary, confidential, and trade secret information through IPC's Salesforce.com database with much greater frequency than he had done during the course of the rest of his employment.

57.

Upon information and belief, Defendant has become employed by, or is about to become employed by, Siemens and is or will be responsible for sales nationwide.

58.

Following the end of Defendant's employment with IPC, IPC demanded Defendant return any and all information obtained from his employment with IPC, but Defendant has failed and refused to do so.

59.

Since Defendant's departure from IPC, upon information and belief, Defendant has been using information and trade secrets that he misappropriated from IPC to unfairly compete with IPC, which IPC acquired and has continued to develop over many years and at a great expense.

60.

IPC has not authorized Defendant to disclose any of the confidential or proprietary information or trade secrets owned by IPC, including, without limitation, the information contained in the Report and the information Defendant printed and downloaded from his IPC-issued computer.

61.

All of this information would be extremely valuable to a competitor and would provide a competitor with an unfair advantage in its sales and marketing efforts toward IPC's customers and prospects.

Defendant's Recruitment of IPC's Employees for a Competitor During his Employment with IPC

62.

Upon information and belief, while Defendant was still employed by IPC, he recruited IPC employees to join him at Siemens.

63.

Defendant's improper activities have thus caused substantial damages to IPC, which are far and in excess of $75,000.

COUNT I

(Action for Misappropriation of Trade Secrets)

64.

IPC repeats and realleges each and every allegation set forth in paragraphs 1 through 63 as if fully set forth herein.

65.

IPC has trade secrets, as described above, which derive independent economic value from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from their disclosure or use.

66.

IPC's trade secrets have been the subject of reasonable efforts to maintain their secrecy.

67.

Defendant has misappropriated IPC's trade secrets by improper means within the meaning of O.C.G.A. § 10-1-761.

68.

IPC has suffered and will continue to suffer actual damages caused by Defendant's misappropriation of its trade secrets, and Defendant has been unjustly enriched by his misappropriation of IPC's trade secrets.

69.

Defendant's misappropriation of IPC's trade secrets is willful, wanton, reckless and malicious, entitling IPC to an award of exemplary damages in an amount authorized by O.C.G.A. § 10-1-763(b).

70.

Pursuant to O.C.G.A. § 10-1-764, IPC is entitled to an award of its attorneys' fees and costs incurred in this action because Defendant has willfully and maliciously misappropriated the trade secrets of IPC, knowing them to be trade secrets.

COUNT II

(Action for Violations of the Computer Fraud and Abuse Act)

71.

IPC repeats and realleges each and every allegation set forth in paragraphs 1 through 70 as if fully set forth herein.

72.

Defendant acquired IPC's information and trade secrets by intentionally accessing, without IPC's authority, a protected computer or protected computer network owned by IPC, through which IPC provides electronic communication services to its employees and authorized users throughout the United States, and on which IPC stores highly confidential and proprietary information and other electronic information and communications.

73.

Defendant wrongfully obtained IPC's information while it was in electronic storage on IPC's protected computers or protected computer network for the purpose of using the information to compete against IPC.

74.

By the foregoing actions, Defendant intentionally exceeded any authorized access to IPC's protected computers or protected computer network, and thereby

obtained information belonging to IPC which was stored on IPC's computers involved in interstate or foreign communication.

75.

Defendant intentionally exceeded any authorized access to IPC's protected computers or protected computer network, and by means of such conduct furthered his intended fraud and obtained IPC's information, the value of which exceeds $5,000 per annum.

76.

By his foregoing actions, Defendant intentionally accessed IPC's protected computers without authorization, and as a result of such conduct, caused and is causing, or recklessly caused and is causing, damage and loss to IPC that exceeds $5,000 in value.

77.

The actions of Defendant constitute violations of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4), and 1030(a)(5).

78.

The conduct of Defendant has proximately caused and is causing damage, loss and other injury to IPC and its property exceeding $5,000 per annum, and IPC

may therefore pursue civil relief against Defendant pursuant to 18 U.S.C. § 1030(g).

COUNT III

(Action for Violations of the Stored Communications Act)

79.

IPC repeats and realleges each and every allegation set forth in paragraphs 1 through 78 as if fully set forth herein.

80.

Defendant acquired IPC's information and trade secrets by intentionally accessing, without IPC's authority, a protected computer or protected computer network owned by IPC, through which IPC provides electronic communication service to its employees and authorized users, and on which IPC stored information and other electronic communications. Defendant wrongfully obtained IPC's information and trade secrets while said information was in electronic storage in said computers or computer systems.

81.

Defendant exceeded any authorization to access the information.

82.

Defendant's actions constitute unlawful access to stored communications and violations of the Stored Communications Act, 18 U.S.C. § 2701.

83.

Defendant's conduct has proximately caused and is causing injury to IPC and its property, and IPC may therefore pursue civil relief against Defendant pursuant to 18 U.S.C. § 2707.

COUNT IV

(Action for Violation of Georgia's Computer Systems Protection Act)

84.

IPC repeats and realleges each and every allegation set forth in paragraphs 1 through 83 as if fully set forth herein.

85.

IPC's computers and computer systems constitute a "computer" as that term is defined by O.C.G.A. section 16-9-92.

86.

IPC's computers, computer terminals, servers, and related devices and software constitute a "computer network" as that term is defined by O.C.G.A. section 16-9-92.

87.

Defendant's use of IPC's computers and computer networks to obtain confidential information, trade secrets and other property of IPC was "without authority," as that term is defined by O.C.G.A. section 16-9-92.

88.

Defendant, through his actions as described above, used IPC's computers and computer networks with knowledge that such use was without authority, and with the intention of taking or appropriating the property of IPC, in violation of O.C.G.A. section 16-9-93(a)(1).

89.

Defendant, through his actions as described above, used IPC's computers and computer networks with knowledge that such use was without authority, and with the intention of obtaining IPC's property by deceitful means and/or artful practice, in violation of O.C.G.A. section 16-9-93(a)(2).

90.

Defendant, through his actions as described above, used IPC's computers and computer networks with knowledge that such use was without authority, and with the intention of converting IPC's property to his own use in violation of

known legal obligations to make a specified application or disposition of IPC's property, in violation of O.C.G.A. section 16-9-93(a)(3).

91.

IPC has been injured by reason of Defendant's individual and collective violations of O.C.G.A. sections 16-9-93(a)(1), (2), and (3) and is entitled to an award of compensatory damages against Defendant, in an amount to be determined at trial.

92.

Defendant's violations of O.C.G.A. sections 16-9-93(a)(1), (2), and (3) exhibit willful misconduct, malice, fraud, wantonness, oppression, or that entire want of care that would raise the presumption of conscious indifference to consequences, such that IPC is entitled to punitive damages in an amount not less than $500,000.

COUNT V

(Action for Breach of Employee Duty of Loyalty)

93.

IPC repeats and realleges each and every allegation set forth in paragraphs 1 through 92 as if fully set forth herein.

94.

As an employee of IPC, Defendant owed IPC a duty of loyalty, good faith, and trust, which included, but was not limited to, a duty not to misappropriate and disclose IPC trade secrets and confidential information. Moreover, Defendant had a duty while employed by IPC to act in IPC's best interest and refrain from engaging in conduct detrimental to IPC.

95.

Defendant breached these duties by misappropriating confidential and proprietary trade secrets of IPC and using such information for his own business purposes.

96.

Defendant also breached these duties by attempting to recruit IPC employees to become employees of Siemens while Defendant was still employed by IPC.

97.

As a direct and proximate result of Defendant's disloyal and unlawful conduct, IPC has suffered and continues to suffer damages.

98.

IPC is entitled to an award of any and all damages caused by Defendant's breach of his fiduciary duty and duty of loyalty, the exact amount of which will be demonstrated and proved at the time of trial.

99.

Defendant's conduct exhibits willful misconduct, malice, fraud, wantonness, oppression, or that entire want of care that would raise the presumption of conscious indifference to consequences, such that IPC is entitled to punitive damages in an amount not less than $100,000.

100.

The breach of duty of loyalty by Defendant caused IPC to suffer damages.

COUNT VI

(Action for Unjust Enrichment against Defendant)

101.

IPC repeats and realleges each and every allegation set forth in paragraphs 1 through 100 as if fully set forth herein.

102.

IPC is the sole owner of its information and trade secrets.

103.

Upon information and belief, Defendant is using IPC's information and trade secrets for his own benefit, gain and advantage, to unfairly compete with IPC.

104.

Defendant has not paid IPC any compensation in the form of royalties or other payments for his use and exploitation of IPC's information and trade secrets.

105.

It would be inequitable and unjust for Defendant to retain the benefits, gains, and advantages resulting from his use and exploitation of IPC's information and trade secrets.

106.

Therefore, Defendant should not in equity and good conscience be permitted to retain the benefits, gains, and advantages resulting from his use and exploitation of IPC's information and trade secrets.

107.

Accordingly, Defendant is liable to IPC for unjust enrichment, in an amount to be determined and proved at the time of trial.

WHERFORE, IPC respectfully prays of this Honorable Court as follows:

(A) For preliminary and permanent injunctive relief restraining Defendant from using in any manner, or otherwise disclosing to any third party, information in his possession, custody, or control which Defendant took from IPC, including IPC's confidential information and trade secrets;

(B) For an order enjoining and restraining Defendant from soliciting business on behalf of Siemens or any other competitor from customers identified on the Report or any of the other documents or information misappropriated by Defendant;

(C) For an order enjoining and restraining Defendant and anyone acting in concert with him from accessing, tampering with, purging, deleting or destroying any tangible or electronically stored information (i.e., whether in hard copy format or contained on computer equipment, electronic storage media, or webmail accounts), which is in his possession, custody or control and which relates in any way to IPC, to any information obtained from IPC, or to their efforts to compete with IPC;

(D) For an order requiring Defendant and anyone acting in concert with him to return to IPC, and make no use of, all confidential information or trade secrets belonging to IPC;

(E) For an order requiring Defendant to immediately provide access to and permit a forensic copy be made by IPC's chosen ESI vendor of all computers (including but not limited to iPads or similar tablets), Personal Digital Assistants, mobile e-mail or smartphone devices (including but not limited to Blackberries, cellular phones, text messaging devices, iPhones, etc.), storage media (including but not limited to flash drives, USB drives, external hard drives, DVDs, CDs, etc.), and e-mail accounts used by Defendant to conduct business or on which any information belonging to, related to or referring to IPC is stored, for the purpose of verifying the return, removal or destruction of all IPC materials and information through a good-faith, mutually agreed upon, third party protocol that will also protect the personal information of Defendant and any employees or independent contractors of Siemens, if any; to the extent that IPC's chosen ESI vendor determines that any computer, storage media or other device covered by the above description cannot be forensically copied on site, IPC's chosen ESI vendor shall be permitted to take such devices for copy at IPC's chosen ESI vendor's site and to be returned to Defendant within 72 hours;

(F) For an order requiring Defendant, to immediately, confidentially provide IPC's chosen ESI vendor with the user name and password of any personal email account used by Defendant and permit access to and a forensic copy to be

made of the contents of any such e-mail account, for the purpose of verifying the return, removal or destruction of all IPC materials and information through a good-faith, mutually agreed upon, third party protocol that will also protect Defendant's personal information, if any;

(G) That IPC be awarded a judgment against Defendant in an amount to be determined and proved at the time of trial;

(H) For an award of IPC's reasonable attorneys' fees and expenses of litigation incurred in pursuing this Complaint;

(I) For such other and further relief as this Court deems just, proper and equitable under the circumstances.

[Signature on following page]

This 14th day of November, 2011.

Respectfully submitted,

BERMAN FINK VAN HORN P.C.

By: *s/ Benjamin I. Fink*
Benjamin I. Fink
Georgia Bar No. 261090
Email: bfink@bfvlaw.com
Matthew J. Simmons
Georgia Bar No. 561107
Email: msimmmons@bfvlaw.com

COUNSEL FOR PLAINTIFF
IPC SYSTEMS, INC.

3423 Piedmont Road, NE
Suite 200
Atlanta, Georgia 30305
Telephone: (404) 261-7711
Facsimile: (404) 233-1943
411132